제1회 한국사이버테러정보전학회 춘계학술발표대회 (2004.5)

협업적 제품거래 서비스를위한 분산 접근제어 프로세서모델

김 형 선*, 박 진 섭**

* ETRI 소프트웨어로봇연구팀, **대전대학교 컴퓨터공학과

요 약

서비스 지향 구조(SOA, Service Oriented Architecture)는 인터넷상에서 구현되는 웹 서비스의 출현으로 인하여 급속도로 발전하고 있으며 활성화 되고 있다. 인터넷환경이 발달함에 따라 분산되어 있는 자원에 쉽게 접근할 수 있고, 시맨틱 웹이란 기술로 보다 광범위하게 지식과 자원을 표현할 수 있다. 그러나 웹 서비스의 사용과 이에 따른 지식과 자원을 보호하기 위해서는 정보보안이 필수 요건이나 웹 서비스의 활성화에 비하여 웹 서비스의 보안 표준이나 웹 서비스 보안이 미비한 상태이다. 본 논문에서는 이러한 요건을 충족하기 위하여 협업적 제품거래(CPC, Collaborative Product Commerce) 서비스를 위한 분산 접근제어 프로세서를 제안한다. 각각의 CPC 서비스마다 독립적인 접근제어 프로세서를 설계하기 위하여 기본적으로 사용할 수 있는 웹 서비스 표준과 기본개념에 따라 분산되어 있는 각각의 웹 서비스를 위한 분산 접근제어 프로세서를 설계한다.

Designing a Distributed Access Control Processor Model for Collaborative Product Commerce Services

Hyung sun Park* Jin sup Park**

ABSTRACT

The service oriented architecture (SOA) is gaining more momentum with the advent of Web services on internet. A programmable and machine accessible Web is the vision of many, and might represent a step towards the semantic Web. However, security is a crucial requirement for the serious usage and adoption of the Web services technology. This paper proposes design goals for an distributed access control model for CPC(Collaborative Product Commerce). It then design a processor model for CPC components, along with web services standard and concept that can be used as a basis to design an access control processor independent of a particular CPC service implementation.

1. 서 론

웹 서비스는 전자거래를 하기 위한 플랫폼으로도 사용할 수 있고 글로벌 웹의 하부구조로 조직간 상호 운용성을 제공하고, 웹에 쉽게 접근할 수 있도록 하여준다. 웹 서비스 개념은 웹 애

플리케이션이 인터넷상에서 쉽게 연결할 수 있도록 공통적인 프로토콜을 제공하는 것이다. 서비스 지향 구조(SOA)의 주요 장점은 산업 표준과 인터넷 표준 같은 표준 메커니즘을 제공하는 기본으로 하기 때문에 인터넷과 친근하고, 조직 내에서뿐만 아니라 기업 간 전자 거래인 협업적 제품거래(Collaborative Product Commerce)의 프레임워크 구현에 적절하다. 기업 간 제품거래를 하기 위해서는 필수 인프라인 정보보호에 대한 요구가 절실하기 때문에 협업적 제품거래 서비스를 위하여 분산되어 있는 CPC 서비스에 대한 분산 접근제어가 필요하다.

이를 위한 해결 방안으로 본 논문에서는 협업적 제품거래 프레임워크에서 분산되어 있는 웹 서비스 의 정보보호를 위하여 분산 접근제어 프로세서 모델을 제안한다. 제안한 모델은 첫째로 웹 서비스를 위하여 포괄적이고 광범위하고 통합된 모델 설계를 목표로 한다. 둘째로 웹 서비스를 위하여 일반적인 웹 서비스 표준모델에 기반으로 한 기본이론에 근거하여 웹 서비스를 위한 분산 접근제어 프로세서 모델을 설계 하였다.

본 논문에서는 제안한 모델에 대한 전반적인 개요에 대하여 기술하고, 2장에서는 관련연구에 대하여 살펴보고, 3장에서는 협업적 제품거래의 웹 서비스 구조에 대하여 살펴보고, 4장에서는 분산 환경에서의 CPC 서비스 모델을, 5장에서는 CPC 웹 서비스를 위하여 제안한 분산 접근제어 모델에 대하여 설명하고, 6장에서 결론을 맺는다.

2. 관련연구

인터넷 환경에서 분산되어 있는 웹 서비스들 간의 접근제어에 대한 연구는 그다지 활발하게 진행되지 않고 있다. Oppliger[8]은 인터넷상에서 웹 서비스에 대한 보안 메카니즘에 대하여 연구하고 있으며, Sandhu와 Samarti[9]는 웹 서비스에 대한 접근제어 원리와 모델에 대하여 연구중에 있고, 역할 기반 접근제어에 대한 견고한 배경 이론을 제공하고 있다. 따라서 본 논문에서는 분산 접근제어 프로세서 설계를 위한 기초로써 위에서 주창한 역할 기반 접근제어 원리들을 사용하여 설계한다.

3. 협업적 제품거래의 웹서비스 구조

본 장에서는 인터넷 환경에서 기업 간 제품정보 공유 및 교환 시 제품정보에 대한 정보보호 기능을 제공하고자 CPC 서비스를 위한 분산 접근제어 아키텍처를 설명한다[1][10].

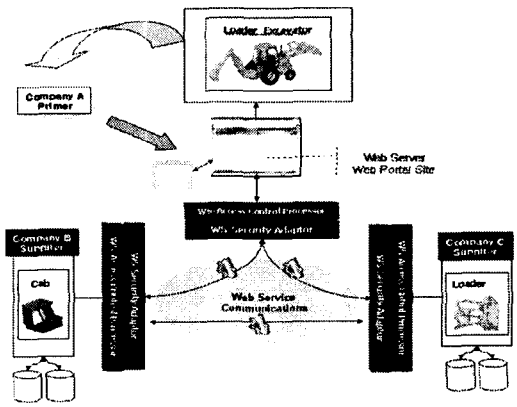

그림 1. 협업적 제품거래의 아키텍처

그림 1에서 보는 바와 같이 분산 환경에서 Primer와 다수의 Supplier들이 제품정보를 서로 공유하고 교환하기 위해서는 웹 서비스 기반 어댑터를 구현하여 분산된 리가시 시스템, 즉 Primer의 시스템과 다수의 Supplier 시스템과 SOAP 통신을 통하여 XML SOAP Message로 제품정보를 주고받는 구조이다. 이때 기업 간 제품정보를 주고받을 때 제품정보를 보호하기 위하여 웹 서비스 어댑터에 접근제어 프로세서를 구현하여 기업 간 제품거래를 교환/공유하는 모든 사용자에게 접근 권한을 부여한다[3].

4. 분산 환경에서의 CPC 서비스 모델

CPC 서비스 모델은 분산되어 있는 일반적인 웹 서비스 모델을 기반으로 접근제어 프로세서를 참조하여 CPC 서비스들 간의 합성뿐만 아니라 기본적으로 CPC 서비스들 간의 합성된 웹 서비스를 결합하여 다시 CPC 서비스의 모음(collection)을 만들어서 분산되어 있는 각각 CPC 서비스의 접근제어가 가능하도록 구성하였다[2][8]. 구성된 CPC 서비스 모델은 다음과 같다.

4.1 CPC 서비스 객체 정의

CPC 서비스 객체는 인터넷상에서 접근할 수 있도록 웹 서비스로 구현하며, CPC 서비스 간에 메시지를 상호 교환하는 컴포넌트로 구현한다.

정의 1 : 하나의 CPC 서비스 객체는 $o=(i,b,l,\Sigma,F,C,M,A)$의 형태로 정의할 수 있다.

(그림 2 참조).

4.2 CPC 서비스 메소드(Mechod) 정의

CPC 서비스 메소드는 CPC 서비스 객체의 한 구성요소로써 다른 CPC 서비스를 호출하여 결과 값을 가져오는 동작을 하는 컴포넌트이다.

정의 2 : CPC 서비스 메소드 $m=(i,o,p,r(p),\mathbb{M})$의 형태로 정의할 수 있다(그림 2 참조).

CPC 서비스 메소드 m은 CPC 서비스 객체 o의 구성요소가 되어야 하고, $\exists o \mid m \in o.F$ 와 같이 표현 할 수 있다.

4.3 CPC 서비스 컬렉션(Collection) 정의

CPC 서비스 컬렉션(collection)은 CPC 서비스 객체들로 구성되어 있으며, CPC 서비스 컬렉션의 계층적인 구조를 이용하여 데이터를 하부구조로 전달함으로써 권한부여 명세와 메타데이터 관리를 쉽게 하기 위하여 CPC 서비스 객체를 합성하는 방법을 제공한다.

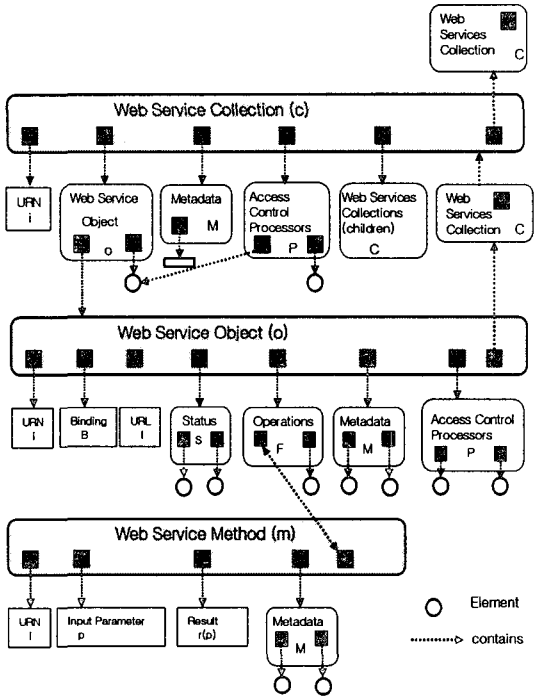

그림 2. CPC 서비스 객체, 메소드, 컬렉션 구조

정의 3 : CPC 서비스 컬렉션(collection) $c=(i,O,C_{CHILDREN},P,\mathbb{M},A)$으로 정의할 수 있다 (그림2 참조).

CPC 서비스 컬렉션은 CPC 서비스 객체와 다른 CPC 서비스 컬렉션으로 구성되는데, 루트가 항상 CPC 서비스 객체가 되는 트리 형태로 구성되어 있다.

4.3 CPC 서비스 합성 정의

하나의 CPC 서비스는 다른 CPC 서비스와 합성하여 새로운 CPC 서비스를 생성할 수 있다. CPC 서비스 컬렉션은 웹 서비스 객체의 컨테이

너로써 사용하였고, CPC 서비스 합성은 CPC 서비스 객체의 CPC 서비스 메소드 간의 동작을 표현한다.

f() = o_1.F.f 는 CPC 서비스 객체 o_1 에 속해 있는 CPC 서비스 메소드이고 , g() = o_2.F.g는 CPC 서비스 객체 o2 에 속해 있는 CPC 서비스 메소드이다. 그러므로 웹 서비스 메소드 f()와 g()의 CPC 서비스 합성을 f*g 형태로 나타하면 (f*g)(a)=f(g(a))로 나타 낼 수 있다.

> 정의 4 : CPC 서비스 합성(composition)은 CPC 서비스 메소드의 o_m.F.f와 o_n.F.f의 합성 결과는 새로운 CPC 서비스 객체 o_k = (i,b,l, Σ, F, C, M, A) 이다. 이때 접근제어 프로세서의 집합은 o_k.A ∪ o_m.A ∪ o_n.A로 정의할 수 있다.

5. CPC 서비스의 분산접근제어 프로세서

분산 접근제어 프로세서를 기반으로 하여 권한부여 구조를 설명한다. 제안된 아키텍쳐에서 분산 접근 제어 프로세서는 두 개의 컴포넌트로 구성된다[5].

- ▶ 접근제어 프로세서 : 접근제어 프로세서는 CPC 서비스 컴포넌트를 위하여 다른 접근 제어 프로세서와 함께 권한부여 결정을 하는 CPC 서비스 객체이다.
- ▶ 케이트키퍼(gatekeeper) : 게이트키퍼는 CPC 서비스 컴포넌트를 위한 개개의 요구를 허용할 것인지 부인할 것인지를 최종 결정 하는 접근제어 프로세서이다.

CPC 서비스 객체를 구현하기 위한 개념적인 모델은 XML, SOAP WSDL 같은 국제표준을 준수해야 하고, tightly coupled 이 느슨한 구조(loosely coupled)인 개방형 웹 서비스 구조로 구현해야 한다. 다음 그림은 분산 접근제어 프로세서 구조를 도시하였다[6][7].

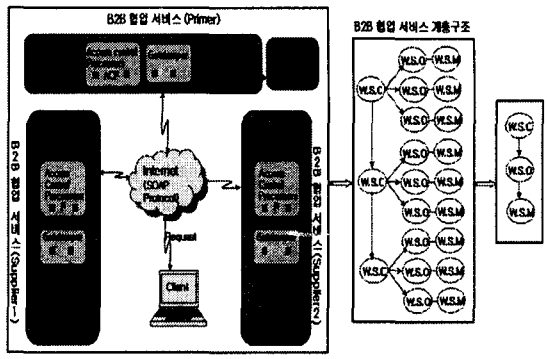

그림 3. 분산 접근제어 프로세서 구조

위의 분산 접근제어 프로세서의 수행되는 시나리오를 설명하면 클라이언트가 Supplier2의 CPC 서비스에 제품정보를 얻고자 엑세스를 시도한다. Supplier1과 Supplier2의 CPC 서비스의 객체의 접근제어 프로세서와 게이트키퍼는 Primer 의 CPC 서비스 컬렉션의 구성원이기 때문에 Primer 의 CPC 서비스 객체에 통제를 받는다. Supplier2의 게이트키퍼는 즉각적으로 클라이언트의 SOAP Message를 차단하여 Primer의 ACP(접근제어 프로세서)와 Supplier2의 ACP는 권한부여 결정 정책을 계산하여 S_{ACL}을 결정한다. 다음 Primer의 게이트키퍼는 Supplier2의 게이트키퍼에게 접근을 허가 혹은 부인을 알려주고, Supplier2의 게이트키퍼는 클라이언트에게 SOAP Message로 되돌려 준다.

5.1 권한부여 결정 (Authorization Decision)

각각의 CPC 서비스 객체는 권한부여를 결정할 수 있는 결정자 역할을 가지고, 각 CPC 서비스 객체의 모든 접근제어 프로세서를 합성할 수 있다. 예를 들면 CPC 서비스 객체 o가 어떠한

웹 서비스 컬렉션의 구성원으로 속해 있지 않다면 단독으로 o.A이다. 반대로 CPC 서비스 객체 o 가 웹 서비스 컬렉션의 자식으로 속해 있다면 o.A ∪ c.A 이다.

CPC 서비스 객체 o를 위하여 권한 부여 결정자 S_{ACL}을 결정하는 개략적인 알고리즘은 아래와 같다.

정의 5 : 권한부여 결정자(Decision Maker)

```
CPC_WebSevice(WebServiceObject o) {
sacp = o.A + unionACP(o.c)
return sacp/*접근제어 프로세서*/
}
unionACP (WebserviceCollection) {
uacps = null;
if (c==null) {
return null; }
else {
uacps = c.A + unionACP(c.P);
} return uacps
}
```

5.2 게이트키퍼의 임무

게이트키퍼의 첫째 임무는 사용자에 대한 인증이며, 인증된 후에 인증된 사용자는 인증 티켓을 발급하여 인증서버에 보내고, 같은 사용자가 CPC 서비스에 액세스 할 때에는 재 인증 없이 접근제어 프로세서가 그 정보를 재사용 한다.

둘째 임무는 CPC 서비스 객체를 위하여 권한부여 결정자의 집합인 S_{ACL}를 결정한다.

게이트키퍼는 CPC 서비스로 들어오는 SOAP Message의 권한부여 요구로 표현된 사용자(principal), 접근자원(resource), 행위 (action), 조건(condition) 등을 분석하여 권한을 부여한다.

5.3 분산접근제어 프로세서와 게이트키퍼

접근제어 프로세서는 CPC 서비스 객체의 게이트키퍼로부터 SOAP Message에 내포한 권한부여 요구사항을 받고, 권한부여 결정을 하고, 권한 부여한 결과는 게이트키퍼에게 되돌려 준다.

정의 6 : 접근제어 프로세서의 정의

모든 CPC 서비스 컬렉션과 CPC 서비스 객체를 R이라고 하면 $r \in R$ 이고, $U = \{r|o \in r.A$ 가 성립된다. $D \subseteq U$ 라고 하면 접근제어 프로세서(ACP)는 a = (o, D, AUTH) 이다. (D : CPC 서비스 객체의 도메인, AUTH : 권한부여 정책(예 XACML))

게이트키퍼는 CPC 서비스 객체로 들어오는 요구에 따라 사용자를 인증하고, 각 CPC 서비스 객체와 관련된 권한부여 결정자의 집합을 결정하여 최종 권한부여를 결정한다.

6. 결 론

지금까지 본 논문에서 협업적 제품거래 웹 서비스에서의 기업 간 제품정보의 교환 및 공유를 위해 발생할 수 있는 보안 문제를 해결하기 위해 분산접근제어 프로세서를 소개하였다.

본 논문에서는 계층적 구조의 CPC 서비스 아키텍처를 도입하였고, 제안한 분산 접근제어 아키텍처는 CPC 서비스 일반적인 모델을 사용하여 CPC 서비스 객체를 구현하여 CPC 서비스 객체간의 상호운용성을 강조 하였다. 또한 B2B 전자거래인 협업적 제품거래에서 분산되어 있는 각각의 CPC 웹 서비스에 접근제어 프로세서를 상하관계를 두어 트리형태로 구현하였기 때문에 누구든지 중요한 제품정보에 접근허용을 할 수 없게끔 다중으로 접근을 통제 하였다. 앞으로는 연구는 새로운 알고리즘의 추가를 통해 더욱 강력한 보안 기능을 제공할 수 있도록 연구 중에 있다.

참고문헌

[1] E. Damiani, S. D. C. di Vimercati, S.Parab oschi, and P. Samarati. Design andof an a ccess control processor for XML docume nts. *ComputerNetworks*,33(1-6):59-75,June 2 000.

[2] E. Damiani, S. D. C. di Vimercati, S. Para boschi, and P.Samarati. Finegrained access control for soape-services. *WWW10*, May 2001.

[3] M. Kudo and S. Hada. XML documentsecu rity based on provisional authorization . *C CS'00*, 2000. IBM TokyoResearch Laborator y. protocol for remotecollaborative authorin g on the Web.2001.

[4] Michiharu Kudo, Satoshi Hada, "XMLDocu mentSecurity based on Provisional Authoriz ation", ACM 2000, pp87-96. 2000

[5] R. Anderson. *Security Engineering: A Gui de to Building Dependable Distributedsyst ems*. Wiley Computer Publishing,2001.

[6] R. Kraft. A model for network serviceson t he web. *The 3rdInternational Conference on internet Computing (IC2002)*, 3:536-541, Ju ne 2002.

[7] R. Kraft. Research and design issues ofacc ess control for network services onthe we b. *The 3rdInternational Conference on Inte rnet Computing (IC2002)*, 3:542-548, June 2002.

[8] R. Oppliger. Methods of securing applications for the world wide *web(WWW).Computer Security Journal,*

[9] R.Sandhu and P. Samarati. Access control: Principles and practice. *IEEE Communications* pages 40-48, September

[10] OASIS, "Web Service Security Core Specification", 2003

김 형 선

1982년 상지대학교 경제학과(공학사)
1992년 광운대학교 컴퓨터공학과(공학석사)
2004년 대전대학교 컴퓨터공학부(공학박사)
1985년 ~ 현재 한국전자통신연구원, 지능형 로봇연구단, 소프트로봇연구팀, 책임연구원

박 진 섭

1981년 중앙대학교 컴퓨터공학과(공학사)
1983년 중앙대학교 컴퓨터공학과(공학석사)
1993년 중앙대학교 컴퓨터공학부(공학박사)
1985년 ~ 현재 대전대학교 공과대학 컴퓨터공학과 정교수